UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,017	07/25/2003	John Mendonca	200209600-1	3688

22879 7590 04/20/2011

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
04/20/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JOHN MENDONCA and AMIT RAIKAR

Appeal 2009-012534
Application 10/627,017
Technology Center 2400

Before RICHARD TORCZON, KARL D. EASTHOM, and STEPHEN C. SIU, Administrative Patent Judges.

EASTHOM, Administrative Patent Judge.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134 from the rejection of claims 1-20. (App. Br. 3.) We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

The Disclosed Invention

The disclosed invention includes a dynamic data center comprising a controller, a graphical user interface, a plurality of internal networks, and a pool of detection intrusion systems. (Spec. 5:19-26; Figure 1.) In operation, "a plurality of monitoring points to be monitored on a network with any of the network intrusion detection systems in the network intrusion detection systems pool 70 are received." (Spec. 8:1-5; Figure 2.) Next, the "controller 10 automatically arranges the monitoring of the monitoring points using the network intrusion detection systems in the network intrusion detection systems pool 70." (Spec. 8:9-11; Figure 2.)

Exemplary claim 1 follows:

1. A method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:

providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;

receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and

automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

The Examiner rejected claims 1-20 as anticipated by Shanklin, US 6,578,147 (Jun. 10, 2003) under 35 U.S.C. § 102(e).

ISSUE

Appellants' responses to the Examiner's positions present the following issue:

Did the Examiner establish that Shanklin discloses the step of "receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems," as recited in independent claim 1, and as similarly recited in independent claims 8 and 15?

FINDINGS OF FACT (FF)

Shanklin

Shanklin discloses "a method for detecting unauthorized access on a network as indicated by signature analysis of packet traffic on the network." (Col. 1, ll. 63-65.) "A plurality of intrusion detection sensors are connected at a network entry point associated with an internetworking device, such as a router or switch." (Col. 1, l. 65 – col. 2, l. 1; FIG. 2.) The internetworking device "includes load balancing programming, which controls how packets are distributed from the internetworking device to the sensors for processing." (Col. 2, ll. 55-58.)

Shanklin's system inspects incoming packets to local network 10 from an external network using IDS sensors 21 attached to a router 22. (See Fig. 2.) Each sensor processes data in multiple protocols to "cover most internet traffic." (Col. 4, ll. 25-28.) The sensors perform packet "signature" analysis, which may involve packet header or payload analysis and/or

packet-by-packet comparisons, to determine if an unauthorized intrusion occurs. (Col. 4, l. 43 to col. 5, l. 7.) A load balancer in the router distributes the packets among the various sensors which are connected in parallel, either on a session-by-session basis (Fig. 2) or a packet-by-packet basis (Fig. 3) (Col. 5, ll. 14-22.)

PRINCIPLES OF LAW

The Examiner bears an initial burden of factually supporting an articulated rejection. In re Oetiker, 977 F.2d 1443 (Fed. Cir. 1992). "It is axiomatic that anticipation of a claim under § 102 can be found if the prior art reference discloses every element of the claim." In re King, 801 F.2d 1324, 1326 (Fed. Cir. 1986).

ANALYSIS

Appellants correctly and generally assert that claim 1 requires the step of "receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems," with independent claims 8 and 15 each reciting a similar limitation. (App. Br. 8.) Appellants maintain that Shanklin fails to disclose "a plurality of monitoring points to be monitored." (App. Br. 10.) Appellants observe that Shanklin's system distributes sessions and packets to "each sensor" (App. Br. 9) and to "all sensors" (id. at 10), but it is not clear how this observation about sensors relates to the argument that Shanklin does not disclose "a plurality of monitoring points to be monitored."

The Examiner generally finds that Shanklin's "'multiple intrusion detection sensors' [IDS] . . . comprise the function of the claimed plurality

of network intrusion detection system, monitoring points and monitoring policy." (Ans. 5.) In other words, the Examiner apparently relies on Shanklin's IDS sensors at each router port (see Figure 2) to satisfy the limitation of receiving a plurality of monitoring points (i.e., IDS sensors in the system receive data – i.e., receive "monitoring points") from different network source points.

Based on the record, the router (22, 32) in Shanklin's system (see Figs. 2, 3) receives signals for monitoring data from different points in the external network on a session-by-session or packet-by-packet basis. Different sessions imply that multiple packets from different sources are monitored at each IDS sensor. In any event, Shanklin's IDS system must monitor different external network source points because it determines which of these disparate network sources are authorized or unauthorized. Also, each IDS sensor handles different protocols in the network, and the system provides load balancing, further implying multiple external monitored sources. (FF, see also Shanklin Figs. 2, 3.)

As such, Appellants' arguments are not persuasive. Appellants have not demonstrated that Shanklin fails to disclose "a plurality of monitoring points to be monitored." As discussed supra, IDS sensors receive "a plurality of monitoring points" (i.e., data representing different network monitored points) from the network. Shanklin's system monitors this plurality "with any of said network intrusion detection systems" as set forth in claim 1. For example, according to Appellants, and assuming for the sake of argument that Appellant is correct, Shanklin's router sends packets or

sessions to "each" and "all" IDS sensors (see discussion supra and App. Br. 9, 10).[1]

Therefore, we will sustain Examiner's rejection of independent claims 1, 8, and 15, and claims 2-7, 9-14, and 16-20 dependent therefrom, because Appellant does not present separate arguments therefore.

DECISION

We affirm the Examiner's decision rejecting claims 1-20.

No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

ak

[1] The term "any" is defined as follows: "1. One or some, regardless of sort, quantity, or number." *Webster's New Riverside University Dictionary* 115 (1984).